The importance of a comprehensive security strategy in enterprise IT solutions

technology brief

Abstract

Breaches of computing security have become a costly menace to information infrastructure and continue to be an ongoing threat to any enterprise and IT organization. Efforts spent defending against Internet-borne attacks have cost billions of dollars in the last five years, and these destructive threats will become more sophisticated and difficult to defend against in the future.

This brief discusses many security-related products and technologies developed to ”bolt-on” to existing infrastructures to protect computer systems from intrusion or theft. In the context of this discussion, the term bolt-on refers to a complementary security technology working to enhance an existing IT environment without being part of the core architecture. Security features built into HP products and solutions increase the effectiveness of the after market bolt-on solutions and provide a computing solution that meets the requirements for a secure environment.

Specific topics covered in this brief include current security threats to IT infrastructure, importance and key objectives of a comprehensive security solution, different levels of security technology, and how IT solutions from HP can address different levels of security threats. While this brief is primarily for the technology professional with an understanding of IT infrastructure, management will also gain insight into the business value of a secure IT environment.

Introduction

As the use of information becomes more valuable and strategic worldwide, the systems that carry this information (IT infrastructure and processes along with the Internet) increasingly become targets for security breaches. Prior to 2001, threats to security included hackers, Disk Operating System (DOS) interpreted viruses, and similar problems resulting in occasional security breaches. However, in today’s environment, security issues are both more prevalent and more malicious in their potential damage. Targeted attacks on IT systems, economic espionage, technology-based terrorism, and disgruntled employees are some of the ever-present threats.

For example, computer viruses are an ongoing threat as they proliferate, with constantly evolving strains that increase in complexity and the potential damage they can cause. In the future, more sophisticated threats, including ”super” worms, polymorphic code, application-level attacks, and massively distributed attacks, are expected to cause even more severe damage. [1] In the aftermath of the September 11, 2001, attacks on the United States, cyber terrorism is now seen as a very real and dangerous threat. As a result, the need for comprehensive security solutions has never been greater for commercial, financial, government, and personal computing environments.

The economic impact of security issues is also growing at an alarming rate, according to the "2002 Computer Crime and Security Survey" conducted by the Computer Security Institute (CSI) along with the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad.[2] This survey, based on responses from more than 500 security professionals in U.S. corporations, government agencies, financial institutions, medical institutions, and universities, articulates the accelerating threat from computer crime and other information security breaches along with an increasing financial toll. Highlights of the survey include the following security issues:

- Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.
- Eighty percent acknowledged financial losses due to computer breaches.
- Forty-four percent were able to quantify their financial losses at more than $455 million.

---

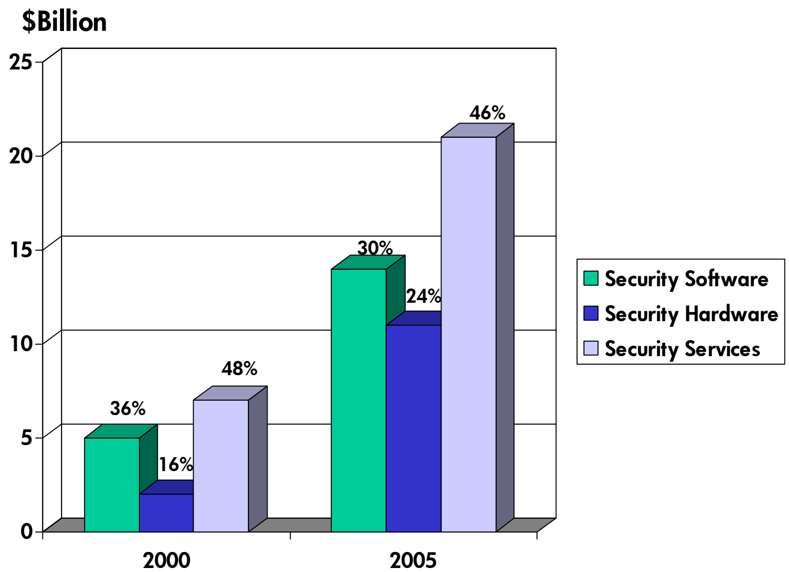
[1] ”InfoSec’s Worst Nightmares,” *Information Security*, November 2002.

[2] ”Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row,” Computer Security Institute, April 7, 2002. www.gocsi.com/press/20020407.html

- As in previous years, the most serious financial losses occurred through theft of proprietary information ($170 million) and financial fraud ($115 million).

Security issues exist across all vertical and horizontal solutions, as can be seen in Figure 1 showing current and future investment in IT security. According to IDC, the annual investment for IT security (comprised of hardware, software, and associated services) was $14 billion in 2000. In 2005, this investment is projected to more than triple to $46 billion.[3] An important trend to note is that security solutions budgets are becoming more services-centric.

Figure 1. Trend in IT security investment



To the casual observer, IT security appears to be solved by using a username and password at the user interface; for example, when one logs onto to a network at work. But in reality, security addresses the entire flow of information and transactions, from the first mouse click to mission critical back-office servers and storage along with their associated networks.

Several misconceptions increase the risk of security violations. Some believe that security is inherent or that security breaches are problems that happen somewhere else. Many people believe their systems are more secure than they really are. For example, although an obscure password or username is helpful, it does not provide a system with sufficient security. Finally, some believe it is faster, easier, and less expensive to implement a solution without security and then to add security later. However, integrating security as part of the original architecture and implementation achieves savings in design, production, and testing.

Three main characteristics of modern computing deliver extensive value to business operations: the prevalence of computers, networking, and remote access. These characteristics also create the greatest challenges to designing a secure environment.

Prevalence of computers at all user levels provides numerous benefits, one of the most powerful being the ability and ease of sharing information. However, once that information is shared, the author has effectively lost control of the content unless strict document control procedures are in place. The user also cannot protect the media or its information if it is lost or stolen. Once information has been

[3] IT Security Study, *International Data Corporation (IDC)*, 2002

shared, gaining access to the information can be as simple as going to any client computer, inserting a form of portable media, and copying files. The obvious issue here is that the owner of the computer would not know that the information was copied, nor could he prevent it from being copied in a typical computing environment. In addition to these issues of information sharing and control, client computer hardware components are readily interchangeable and reusable. While this is desirable for repair, maintenance, and upgrade of systems, it makes tracking computer inventory very difficult and enables a market for stolen hardware.

Companies often network their computers. In fact, it is estimated that more than 50 percent of the world's total computing resources are connected to a network. This connectivity has numerous benefits, as well as issues. Networking makes it easy and efficient to deliver and receive information, leading to increased productivity. But once the information is forwarded, the author has lost control of the information. For example, if a person allows replication of his Lotus Notes database, he cannot prevent someone else from duplicating it elsewhere. A network also provides a replacement for the physical mail system. One can now receive mail in a matter of seconds instead of waiting days. While this capability is very powerful, it is fairly simple to forge e-mail.

Networks must be maintained while running nearly all the time, thus requiring real-time maintenance. For example, a simple computer program can debug, repair, and maintain a large network. While such a program is clearly a very powerful tool, a single person can use this same program to see logins, passwords, and other confidential material on the network. With client/server as the dominant network architecture, critical information continues to become accessible to greater numbers of people.

There is a growing trend to enable remote access to corporate resources through notebook computers, Personal Digital Assistants (PDAs), wireless networking, and telecommuting. This trend also involves the emergence of inter-networked computing. More enterprises and businesses connect their internal networks to the greater network of other businesses and consumers, on the Internet. These interconnected networks enable businesses, suppliers, customers and employees to collaborate more effectively while gaining access to critical systems' resources or information across public, traditionally unsecured networks.

In the inter-networked environments that are most common today, organizations have a strong desire to increase connectivity to reduce time-to-market, increase worker mobility, and increase availability and proliferation of information. However, this must be balanced with sufficient security processes and infrastructure that support a highly connected work environment.

Other potential issues affecting system security are legal implications. Recent United States court cases suggest an emerging precedent of "downstream liability." This precedent requires companies to deploy "reasonable measures" for security or face potential liability for computer attacks launched on other parties from within their network. For example, if someone breaks into the soft security of Company B and uses this trusted position to hack into Business Partner C's more robust security system, Company B could be held legally liable. While U.S. government regulation of computing security continues to evolve, measures are already in place allowing state and federal courts to hold enterprises responsible for the privacy of customer and consumer information.

Elements of security

A secure infrastructure should be designed as a total end-to-end solution, from handheld wireless devices to the servers, and everything in between, including the entire communications framework. In general, a complete security solution must include the following components, referred to as the PAINS model:

- Privacy: Ensuring that only the sender and intended receiver can hear or see what is being communicated.

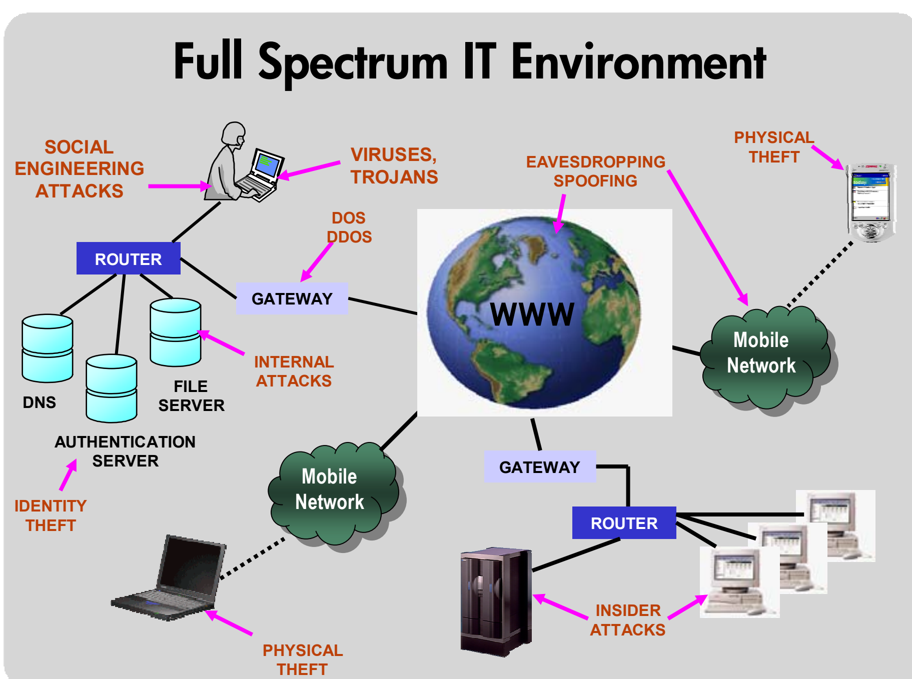
- Authentication: Providing guarantees that the recipient and/or sender are who they claim to be. This also confirms that the message was created by the sender.
- Integrity: Ensuring that messages are arriving in tact and unaltered.
- Non-repudiation: Guaranteeing that a transaction between two clients either did or did not occur. This eliminates or reduces claims that parties did not receive their messages.
- System management: Providing a security system with security policies that are straightforward and user friendly to ensure proper use.

The largest challenge with any security system is the management involved. First of all, if a security system is too invasive or complicated, people will not use it and it will be ineffective. For example, password policies, including user definable and randomly generated passwords, need to be established by IT authorities. Users should typically be authorized for access only to the specific resources they need for their job functions (access control). Regardless of the levels of security employed by the organization, security policies must also be straightforward and user friendly, or they will not be used properly.

Whether developing, upgrading, or maintaining a secure infrastructure, all five of the security components identified above are required for a robust security system. Furthermore, the PAINS model is very important for the growth of the Internet, especially with the continuing growth of e-commerce.

Security also needs to cover the full spectrum of the IT environment, protecting every device and point of access (Figure 2). If security is implemented on a desktop client and a handheld device provides user access into the infrastructure, the same level of security should be implemented on the handheld. Any security solution must be ubiquitous across the entire architecture; if unsecured clients are allowed to access an extremely secure server, security is clearly being compromised. Similarly, putting a firewall in front of web servers does not make them completely secure. This is a point solution and it will not be effective. An attacker will simply find a route around the security point solution.

Figure 2. Full spectrum security



HP security strategy

Through its technological research, industry-specific applications, and industry standards involvement, HP has developed a broad range of security-based solutions for solving even the most challenging security issues. Choosing an optimum solution begins with a holistic approach of evaluating an organization's security needs within the context of its business environment.

Each HP security solution will have a different infrastructure based upon customer needs, the budget, and the level of security required. The foundation of the HP security infrastructure includes three categories of security level criteria that enable system designers to evaluate solutions relative to the cost, ease of use, availability, and robustness of the security solution. Each of the following criteria helps determine how effective or appropriate a solution may be for an individual enterprise:

- Functionality: How complete a solution does the security measure offer? How sophisticated an attack can the security solution withstand?
- Availability/performance: How "available" will the solution be and how will it affect system performance? These criteria measure how well the solution operates against the 24 x 7 standards of modern networks and the transparency of its execution.
- Ease of use/integration: How easy to install, use, modify, and manage is the solution within a platform or enterprise environment? This criterion gauges whether a solution provides security in a way that encourages users and administrators to actually use it, and whether it provides the centralized administrative tools they need to manage the solution. It also measures whether enterprises can integrate the solution seamlessly with an existing product set.

While numerous areas must be addressed for an effective security solution, three overall core security goals must be achieved. The security system must be:

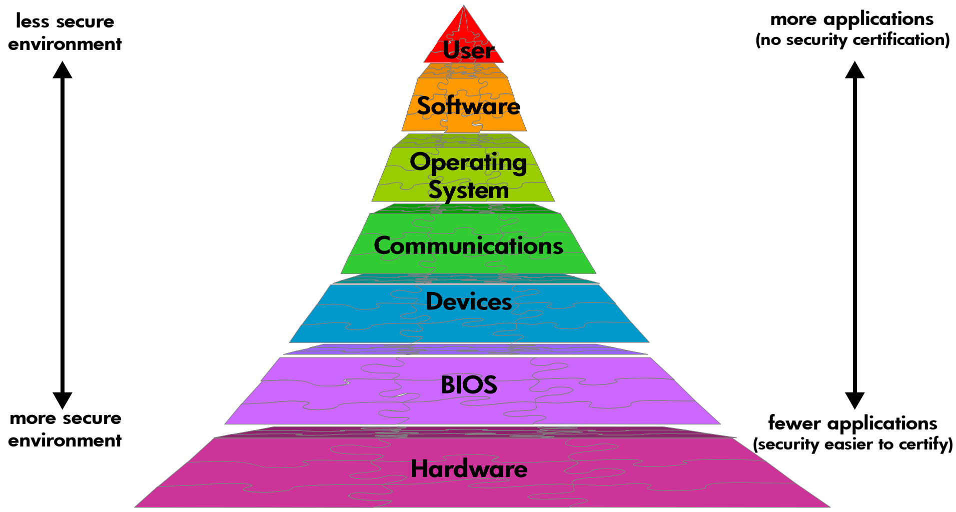
- Ubiquitous (end-to-end): All system areas must be secured. There is little use in having the most secure server if unsecured clients are allowed access.
- Easy to use: An easy-to-use security system proliferates by way of its usability; hence, it becomes more effective. If security systems are too difficult to use, people will simply not use them.
- Easy to manage: Once a secure system is in place and being broadly used, teams must be able to manage and maintain the system. If it is too difficult to manage, it will not be used properly.

For example, most security solutions today typically focus on the communications link in support of the expanding e-business industry. But from the perspective of a total security solution, a secure communications link without secure end nodes is no better than an unsecured link. A more complete security strategy operates in reverse: First secure the end nodes by (1) ensuring they have not been tampered with and (2) validating that the person sitting at the PC is who he claims to be. Then provide a secure (private) communications link with that end node.

The security pyramid

In the information security industry, security trust models are viewed as pyramids (Figure 3). In the context of this discussion, trust is defined as knowing the state of a machine (hardware, software, applications) and making informed decisions about its validity, or the decision of whether the machine has the authority to access the requested environment. The trust pyramid can be viewed as a series of layers through which data must pass, beginning from the bottom and moving up. The ideal security trust model is built upon a strong foundation with no gaps between the layers. If each level of the security model is built using the best security tools, the resulting structure will be strong and able to withstand an attack. If not, the structure is vulnerable to attack.

Figure 3. Traditional security pyramid

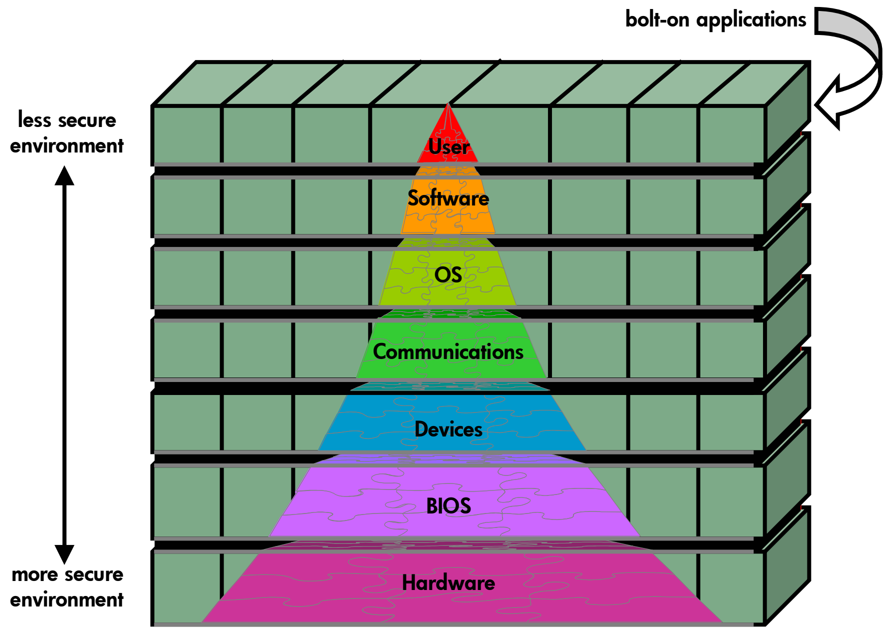


For example, virus-scanner software functions at the software layer and provides protection from software-based viruses. But a virus can be introduced at a lower level of the pyramid—at the Basic Input-Output System (BIOS) level—and will never be seen or caught by the virus scanner. As another example, a hacker could circumvent logon security and boot from a floppy disk to introduce viruses or perform a Read Only Memory (ROM) flash operation to gain password and logon information.

These situations illustrate the importance of securing all layers of the pyramid. HP approaches these problems with an end-to-end strategy, where HP products are designed to fill all these gaps.

Bolt-on/bolt-in security solutions function as walls or barriers attached on either side of the pyramid to extend and support the pyramid structure. They are an important portion of the complete security solution (Figure 4).

Figure 4. Ideal security pyramid with bolt-on products in place



The reality of today's computer security is that while there are good tools available, they have not been tied together to form a complete solution. Gaps or holes still exist in the computer security pyramid through which hackers can gain access. For example, consider encrypted data stored on a disk. If the user merely deleted the original file and created a new, encrypted file, the original file would still exist on the disk. While the user took precautions to secure the data by encrypting it, his efforts were negated by the existence of the original file. A better solution is to write the encrypted file to a new disk and either destroy or thoroughly erase and reformat the old disk.

HP has addressed many of these security gaps with specific technologies or products that will be discussed in the next section. Advanced security solutions include those at the user, software, hardware, BIOS, communications, and device levels.

Security infrastructure components and technologies

As a founding company of the Trusted Computing Group (TCG) and a founding member of its predecessor, the Trusted Computing Platform Alliance (TCPA), HP has taken a leadership role in the industry to integrate security technologies into a common framework. The TCPA was formed in late 1999 as an open, industry-wide alliance focused on improving trust and security on computing platforms. Founded by Compaq, HP, IBM, Intel, and Microsoft, TCPA grew to more than 150 companies who collaborated on hardware, software, communications, and technology issues. Member companies developed and implemented TCPA specifications to create an enhanced hardware and software operating environment. This operating environment was based on a TPM that implemented trust (defined here as an enhanced level of security) into client, server, networking, and communications platforms. In essence, TCPA served as an anchor for system security beyond physical attributes and became an e-business enabler that provided platform integrity and authentication along with protected storage.

As the need for security continues to expand, TCG has superseded the TCPA and is driving security-based standards into the marketplace. While an extensive discussion of TCG and TCPA is beyond the

scope of this document, additional information can be found on the TCG website at www.Trustedcomputinggroup.org and the former TCPA website at www.Trustedcomputing.org.

Key elements of effective security solutions include hardware, software, and education. Current solutions tend to focus on bolt-on products such as virus scanners, firewalls, intrusion detection technology, encryption packages, computer forensics, and BIOS-level protection. While the use of specific bolt-on point solutions described herein addresses pieces of the security landscape, solutions should always be evaluated and chosen based on the entire security infrastructure in relation to business needs.

Hardware

Hardware security features provide a more secure operating environment by limiting or restricting physical access to devices (server chassis, hard drives, client devices, etc.). Hardware security includes a variety of low- and high-tech implementations ranging from component locks that physically secure devices, to high-speed encryption chips that improve server performance of cryptographic operations. This layer of protection is a very important first step in security that must be in place. Examples of hardware security protection include:

- Simple cover lock and key
- Electronically controlled smart cover locks
- Case sensors to provide remote system management software notification of system intrusion
- Cable lock to prevent unwanted configuration changes or component removal
- Drive locks to secure hard drive data
- Tamper-resistant fasteners (screws, bolts, brackets, etc.)

Physical access devices

Access devices protect against physical access or provide notification that something has been accessed. For physical protection, HP installs electromagnetic locks on its ProLiant servers that use the administrative password as a key. For detection, case sensors are used. For user identification and authentication, HP uses both token and biometric technologies. Token devices can be used either alone or in conjunction with another security mechanism to prove the identity of an individual or entity. By contrast, biometrics uses biological characteristics of the user instead of a device for authentication. These will be discussed in greater detail in another section.

Acceleration hardware

Depending on the technologies employed, some security implementations can create processing and network traffic that can degrade the performance of a system. Because of this, a security solution sometimes includes hardware designed to process security-related transactions and thereby accelerate the overall system performance.

Peripheral Component Interconnect (PCI) card based co-processors from Atalla and other vendors accelerate Secure Socket Layer (SSL) cryptographic processing while handling peaks in transaction volumes. For example, without any acceleration hardware, an HP Proliant DL380 dual-processor 1GHz Xeon server is rated at 229 SSL operations per second at 100 percent CPU utilization, or 2.29 ops/sec/1% CPU capacity. With an Atalla AXL600L accelerator card installed in the same server, the performance jumps to 466 SSL operations per second at 68 percent CPU utilization, or 6.85 ops/sec/1% CPU capacity. This results in a 3X server productivity improvement with the AXL600L card installed.

Pre-operating system

In the industry-standard server segment, the pre-operating system (pre-OS) provides security through several attributes including BIOS passwords, remote management capabilities, and state or machine integrity technologies such as pre-OS virus scanners and pre-OS configuration validation. In addition, the Trusted Computing Platform Module (TPM) is used to securely boot the machine in an authenticated mode.

Software applications

Firewall and anti-virus software are the best understood and most developed standalone security solutions on the market, and they continue to mature as products. Recently, several significant new software approaches have emerged that provide for more secure environments; for example, secure operating systems, secure application program interfaces, certificate servers, single sign-on solutions, and middleware. Many recent innovations in cryptography, perhaps the most essential security technology, also focus on software. For its industry-standard server line, HP most commonly uses three types of software-based security products: secure operating systems, virus scanners, and BIOS options.

BIOS options

BIOS options provide access control. For HP's purposes, BIOS level security protects a system from unauthorized access after it is powered on. BIOS level security can include password technology or pre-boot authentication and certification.

Secure operating systems

A secure operating system is one that has undergone formal evaluation to determine if it is secure. In identifying secure operating systems, several assumptions are made; the most important is that the physical machines are not accessible.

Virus scanners

Virus scanner products from McAfee Associates, Norton, Symantec, and other companies provide unique virus scan capability. If the executing program is infected, the software informs the user, prompts for the removal of the virus from the program, or recommends halting the execution of the requested program.

User education

User education is important to the success of any of hardware or software security solutions. Without the knowledge of appropriate security techniques, users cannot design or maintain effective security measures. With education on how to select security technologies, products, and solutions and on what to use when and where, personnel can acquire skills needed to establish appropriate security measures.

Operating system

To ensure a secure system, a critical step is to use security enhanced operating systems (OS). These OSs, typically denoted by an "SE" at the end of their name, have already been evaluated for security vulnerabilities, enhanced with appropriate security functionality, and certified to comply with a recognized government or industry standard. HP offers a broad range of enhanced or certified secure operating systems pre-tested and integrated with its products. These include Microsoft® Windows XP (SE), Windows® 2000 (SE), Windows NT® (SE), WTS (SE), PocketPC (SE), Exchange (SE), and Release Manager for Microsoft Exchange. In addition, HP offers operating systems (HPUX, Tru64, OpenVMS, and Non-Stop Kernel [NSK]) that have security designed into the core architecture.

User access and authentication technologies

Once a device on the system is physically secure and a trusted computer is created, with no viruses installed, the next challenge is to qualify who is sitting in front of the computer. How does one know that the user of this computer is an authorized user and know what this user is authorized to do? For this, authentication is needed.

There are three types of authentication: something the user knows (password or PIN), something the user has (Smartcard or Token), and a physical characteristic of the user (biometrics such as fingerprints, voice recognition, or retinal eye scans). For added security, multiple factors of authentication can be used, such as biometrics and password; password and a smartcard; or password, smartcard, and biometrics.

User IDs and passwords are the typical method for identifying computer users, but these have proven to be cumbersome. Over 60 percent of help desk calls are password related and, at $45 per call for a US-based help desk, an expensive solution. Effective alternative technologies include biometrics, tokens, and smart cards. Each of these will be discussed in the following paragraphs.

With numerous methods available to authenticate users, determining the best solution includes these steps:

- Evaluating the threat model
- Determining what the technology is being used for (network login, transaction authorization, etc.)
- Identifying how information will be obtained and provided to system
- Defining the worst-case scenario (device failure, false positive, false negative)

The information from these steps will help determine the most appropriate security technology.

Biometrics

There are two basic types of biometrics: behavioral and organic. Behavioral biometrics is the way that people talk, walk, or write their names. Since these actions are learned, they can be learned and copied by others. Organic biometrics includes fingerprints and eye color (the color of the iris). These attributes cannot be changed and are very difficult for others to duplicate.

Common biometrics include fingerprints, the eye (iris), face, and voice. These all work but have their own particular problems. The fingerprint is well established and reliable, and iris recognition is a promising, upcoming technology. Face and voice biometrics are less reliable and are either too difficult to implement reliably or too easily affected by external factors. Less common biometrics include signature verification, hand geometry, retinal eye scans, handprints, and facial thermography. Exotic biometric technologies are being evaluated, including Deoxyribonucleic Acid (DNA), walking gait, and brain waves.

Biometrics effectiveness and quality control are measured in terms of false positives and false negatives. False positives, measured as False Accept Rate (FAR), are a breach of security (the system just gave access to an intruder). False negatives, measured as False Reject Rates (FRR,) are most often a user inconvenience. Both are very important aspects of biometrics that should be considered.

HP's biometrics choice for some of its products has been fingerprint authentication. It is a fast and easy login method for end users and eliminates management of forgotten and expiring passwords.

Tokens

Tokens are devices that users can carry with them to be used alone or with other forms of security technology to prove identity. Types of tokens include stored value tokens, cryptographic tokens, and digital signature cards. For these devices, responses include time synchronized, event synchronized, and challenge responses. There are also Universal Serial Bus (USB)-based tokens that plug into a USB port for added convenience.

There are some potential problems in using tokens, including physical security. For example, some tokens are easy to open and reprogram, and communications on the USB connection can be intercepted. It is important to note that USB tokens are not Smartcards, which must conform to specific standards including form factor. However, viable tokens are rated with the FIPS 140-2 standard, which includes four different levels of security. For more information, see http://csrc.nist.gov/cryptval/140-2.htm

Smartcards

Smartcards are a type of token and another authentication solution used by HP. An example of the use of this technology is HP's Protect Tools. A Smartcard includes information that is unique to its owner and can be read by Smartcard readers at system access points. There are two classes of Smartcards: standard and enhanced. Likewise, there are two types of Smartcard readers to meet different customer requirements: normal card readers and enhanced card readers. For standard Smartcards, the keyboard and reader pass the PIN via the computer before sending it to the Smartcard. During this process, the PIN could potentially be intercepted. By contrast, Enhanced Smartcard devices are self-contained and provide a higher level of security because the PIN never leaves the keyboard or reader.

System management

System management is one of the cornerstones of an effective security program, as it is the central "control room" that monitors all security layers. From the standpoint of security, system management includes, but is not limited to, remote management and real-time alerting, chassis intrusion events, and changes in memory configuration (for example, someone removing a memory module). Some specific products from HP that provide remote system management include the Remote Insight Lights-Out Edition (RILOE) and RILOE II management systems along with the Integrated Lights-Out (iLO) Standard and Advanced management systems.

System management also provides password management and schemes, including local accounts with directories turned off, use of both local and directory accounts, and disabling of local accounts. System management security features that should be considered include use of SSL to protect the communication channel, 128-bit encryption of remote consoles, hardware-based random number generator, and use of Public Key Cryptographic System (PKCS) certificate requests and import client certificates.

Network considerations

Once the end node is physically secured and authenticated by the user, the next step is to look at securing the network, or in the case of many organizations, a communications pipeline of many networks. A network typically has different protocols including Local Area Network (LAN), Remote Access Server (RAS), Wireless LAN, Broadband, and Wireless Telephony. Each of these protocols has several transition layers: from the device to the access point, from access point to firewall, and then from the firewall to the local machine. Common security issues that concern networks include snooping, unauthorized packet modifications, and forgery.

In many cases, an effective solution is to implement a Virtual Private Network (VPN) on top of any of these existing networks. VPNs are secure because they are an authenticated session using encrypted transmissions. They add an extra layer of security on top of an existing secure infrastructure. However, if not properly managed, added overhead for encryption can result in performance degradation.

The following sections describe each major communications protocol and identify related security issues.

LANs

With LANs, there are no transition points because the user is already inside the firewall. Paradoxically, the LAN is one of the least secured areas because it is assumed that anyone who has access to the LAN is trusted. Unfortunately, this is not true. Recent FBI statistics show that 67 to 74 percent of all security breaches occur within the firewall. Although there are passwords on the machines, there is generally nothing to stop someone inside an organization from connecting a packet sniffer or other such device to the network.

RAS

RAS is one of the more inherently secure network protocols due to the legal framework for phone lines. It is illegal to tap phones without a court order, and access to central switches is limited. While it is possible to tap into the line outside someone's house, this would be difficult without being seen and requires unique skills to accomplish.

Wireless LAN

While wireless LAN protocols such as Institute of Electrical and Electronics Engineers (IEEE) 802.11b are evolving to become more secure, existing weaknesses must be managed through deployment policies, VPNs on top of 802.11b, and automated key management technology.

Broadband

Asynchronous Data Subscriber Line (ADSL) and Integrated Services Digital Network (ISDN) protocols are point-to-point connections until the access point is reached, and then there is no certain way to ensure that the access point is secure. ADSL will normally go through an Internet Service Provider (ISP) for connection to the Internet; but the question then becomes, "How secure is the ISP?" Both ADSL and ISDN are secure at the phone line, but cable modems are similar to a telephone party line in that one user can monitor another user's messages if there is inadequate firewall protection.

Wireless telephony

Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA) are common cellular telephone services in North America. They provide a digital transport; but because there is no underlying encryption, they can be tapped into. However, since they are digital networks, tapping in would require a digital-to-analog converter on the listening device. Global System for Mobile Communications (GSM) is the cellular standard used in Europe and Asia that incorporates full-length encryption. GSM links are inherently secure due to the underlying encryption. In both cases, once the access point is reached, the data is in the standard phone system and therefore relatively secure.

Protocols

While SSL and Internet Protocol Security (IPSEC) are protocols and not networks, they are important enabling technologies in relation to security. SSL protects the digital communications between a browser (client) and a server (or host) and is the de facto industry standard cryptographic protocol for Internet-based VPNs. Unlike other well-known protocols, such as Secure Electronic Transactions (SET) for credit card transactions over the Internet, SSL does not require a complex architecture to be in place. SSL is deployed in virtually every browser and in millions of web servers around the world. However, system overhead from SSL transactions causes significant hardware demands that can be effectively managed through the use of Atalla technologies (discussed in an earlier section).

IPSEC is another protocol used for VPN connections. Working at the network layer, IPSEC secures the exchange of IP packets and is best suited for site-to-site connections requiring large, constant data transfers. However, it has higher maintenance and deployment requirements than SSL-based VPNs.

Professional services

By now it should be clearly evident that a successful security program is not solely based on specific hardware or software technologies, but rather on a comprehensive understanding of business and system needs. Unless an organization has internal resources with extensive security knowledge, professional services are typically employed to assist with strategic areas like policy creation and management, architectural support, security threat model analysis, security integration monitoring, and response mechanisms. HP has extensive capabilities in these areas to assist organizations with these and other security-related needs.

Conclusion

This technology brief has discussed ubiquitous security solutions that provide protection against a broad range of threats to an organization including:

- Theft, unwanted intrusion, or tampering with the physical hardware
- Unwanted alteration of client or server-based software and configurations
- Unwanted snooping or alteration of critical data on the network or Internet communications pipe
- Fraudulent access and logins (user authentication)
- Access to sensitive information by unauthorized users (access control)

While numerous specific technologies can contribute to a robust and secure environment for any organization, effective information security is ultimately a business decision built upon sound planning and implementation of both policy and technology. Security technology alone is not a solution; it is a component. It is therefore important to identify the desired security solution before selecting specific technologies. Once a security program is in place, it must be monitored, since both technologies and security threats continually evolve.

When given sufficiently high priority, security becomes an integral and effective part of the organization's business case for information management. In this case, security is evaluated with a structured, holistic approach using the PAINS methodology. When the PAINS areas (Privacy, Authentication, Integrity, Non-repudiation and System management) are thoroughly addressed, a complete solution can then be designed with the appropriate use of hardware, software, services, and partners. HP is in a unique position to provide security-based solutions for customers with a broad range of security needs.

Call to action

To help us better understand and meet your needs for ISS technology information, please send comments about this paper to: TechCom@HP.com.

TC030611TB, 06/2003

Printed in the US